METHOD AND APPARATUS FOR SECURE TRANSMISSION OF IDENTIFIER FOR REMOVABLE STORAGE MEDIA

ABSTRACT OF THE DISCLOSURE

A media serial number (MS#) for a removable data storage cartridge (22) is asymmetrically encrypted using a private key (106) from a key list (103) which never leaves the factory. This factory encrypted value (FEMS#) is stored in a secure memory device (46) in the cartridge, along with an identifier (FKI#). A drive (21) can obtain the encrypted value and associated identifier from the memory device, and pass them to a requesting program (76), which has a list (176) that it accesses with the identifier to obtain a public key it then uses to decrypt the information. An additional feature involves a second level of asymmetric encryption using additional lists of public and private keys. Another feature permits the requesting program to include in its request a random number, which is subsequently included with the information encrypted at the second level.